Journal of Diabetes Science and Technology
Volume 4, Issue 2, March 2010

ORIGINAL ARTICLES

A Hazard Analysis for a Generic Insulin Infusion Pump

Yi Zhang, Ph.D., Paul L. Jones, M.S.C.E, and Raoul Jetley, Ph.D.

Abstract

Background:

Researchers at the Food and Drug Administration (FDA)/Center for Device and Radiological Health/Office of Science and Engineering Laboratories have been exploring the concept of model-based engineering as a means for improving the quality of medical device software. Insulin pumps were chosen as a research subject because their design provides the desired degree of research complexity and these types of devices present an ongoing regulatory challenge.

Methods:

Insulin pump hazards and their contributing factors are considered in the context of a highly abstract generic insulin infusion pump (GIIP) model. Hazards were identified by consulting with manufacturers, pump users, and clinicians; by reviewing national and international standards and adverse event reports collected by the FDA; and from workshops sponsored by Diabetes Technology Society. This information has been consolidated in tabular form to facilitate further community analysis and discussion.

Results:

A generic insulin infusion pump model architecture has been established. A fairly comprehensive hazard analysis document, corresponding to the GIIP model, is presented in this article.

Conclusions:

We believe that this work represents the genesis of an insulin pump safety reference standard upon which future insulin pump designs can be based to help ensure a basic level of safety. More interaction with the diabetes community is needed to assure the quality of this safety modeling process.

J Diabetes Sci Technol 2010;4(2):263-283

Author Affiliation: Office of Science and Engineering Laboratories, Center for Device and Radiological Health, U.S. Food and Drug Administration, Silver Spring, Maryland

Abbreviations: (BG) blood glucose, (FDA) Food and Drug Administration, (GIIP) generic insulin infusion pump, (ISO) International Organization for Standardization, (MBE) model-based engineering, (PHA) preliminary hazard analysis

Keywords: hazard analysis, insulin pump, safety

Corresponding Author: Yi Zhang, Office of Science and Engineering Laboratories, Center for Device and Radiological Health, U.S. FDA, 10903 New Hampshire Ave., Silver Spring, MD 20993-002; email address Yi.Zhang2@fda.hhs.gov

Introduction

Insulin pumps play an important role in modern diabetes treatment. These pumps are typically used to help maintain blood glucose (BG) levels by delivering rapid-acting insulin through a catheter placed under the skin. Pumps used for subcutaneous insulin delivery not only provide patients with increased convenience and flexibility, but also provide the potential for greater dose precision, more reliable insulin action, and relatively quick dosing adjustments for different lifestyle activities.[1]

While insulin pump technology has helped patients lead a more normal, healthy life, the devices do present risks (i.e., combination of the probability of occurrence of harm and the severity of that harm[2]) to the patient or user of the device. These risks are rooted in the complex technology itself, development and manufacturing errors, individual differences in physiology and lifestyle, and because the devices are operated by patients themselves, on a daily (24/7) basis, and in diverse environments.

The Manufacturer and User Facility Device Experience database[3] maintained by the U.S. Food and Drug Administration (FDA) indicates that there were over 5000 adverse events reported for insulin pumps in the year 2008. It is imperative that the diabetes community and insulin pump manufacturers work together to comprehensively address foreseeable risks and establish risk control measures (i.e., process in which decisions are made and measures implemented by which risks are reduced to, or maintained within, specified levels[2]) that reduce overall risk to an acceptable level.

We believe it would be helpful to the diabetes community to establish a common insulin pump safety reference model. All stakeholders could use this as a basis for discussing and exchanging information as well as specific concerns about insulin pump safety. This article strives to establish the foundation for such a reference model by identifying hazardous situations and their causes for a notional generic insulin infusion pump. We make no claim that this set of hazardous scenarios or their causes are exhaustive. We encourage users, manufacturers, researchers, and regulators alike to consider them and expand upon them in an open forum.

Background

For several years now, software researchers at the FDA/Center for Device and Radiological Health/Office of Science and Engineering Laboratories have been exploring the concept of model-based engineering (MBE)[4] as a means for manufacturers to develop certifiably dependable/safe medical devices, software, and systems. In MBE, developers use executable models as the primary development artifact for discovering and eliminating design errors early in the life-cycle development process. Infusion pumps were selected as a target for studying MBE methods because their design provides the desired degree of research complexity and these types of devices present an ongoing regulatory challenge. To date, this research has been focused on the development of a generic patient-controlled analgesia infusion pump safety model.[5,6]

In light of the growing incidences of diabetes in our society, we are extending our research to address safety (i.e., freedom from unacceptable risk[2]) issues associated with insulin pumps. This article represents the first step in establishing safety properties for a generic insulin infusion pump (GIIP).

Purpose

The purpose of this article is threefold:

1. To establish a set of safety properties for a GIIP safety model (once this model is complete, clinicians may experiment with it to verify its relevancy in terms of clinical experience and compare it with design features already in place to validate it).

2. To establish a set of safety properties for insulin pumps that may be used as a basis for community discussion and to lay a foundation for developing national or international consensus standards for insulin pump safety.

3. To establish a set of insulin pump safety properties that academics may use in medical device MBE research projects, manufacturers may use as a safety reference, and regulators may reference in assessing the safety of these devices.

To accomplish our purpose we need to understand the types of hazardous situations and their causes arising from insulin pump design/development errors and types of pump use errors. Carrying out a preliminary hazard analysis (PHA) is the first step in this process.

A comprehensive PHA relies on a disciplined, methodical study of device hazardous situations and their causes during the earliest phases of developing a device design. The term preliminary is used because few details may be known about the device until the design architecture and implementation become (more) concrete.

Scope

Safety concerns considered in this article are based on designs generally found in legacy (predicate) devices and devices currently on the market or likely to be on the market in the not too distant future. We identify features common to these devices as part of our generic insulin pump model and intentionally exclude many features being pioneered by specific pump manufacturers, such as embedded glucose meters, built-in infusion sets, and remote controllers. Our work is focused on "standard" electronic personal use insulin pumps with infusion sets only. Hospital use insulin pumps or implanted insulin pumps are not considered in this work. However, because the model is a design abstraction, its safety-related issues can be mapped to any type of insulin delivery device. For example, insulin pumps without an infusion set still have to deliver the drug. In our model this may be accomplished via the infusion-set component shown in **Figure 1**. This component can be implemented as a subcutaneous insulin delivery mechanism that is part of the device versus an external infusion set and reassessed for hazards associated with this design choice.

We have established a system boundary for our insulin pump model as depicted in **Figure 1**—it comprises the GIIP (pump), the user, the infusion set (connection), and the environment. We exclude device accessories such as glucose meters, the infusion sets themselves, and remote controllers.

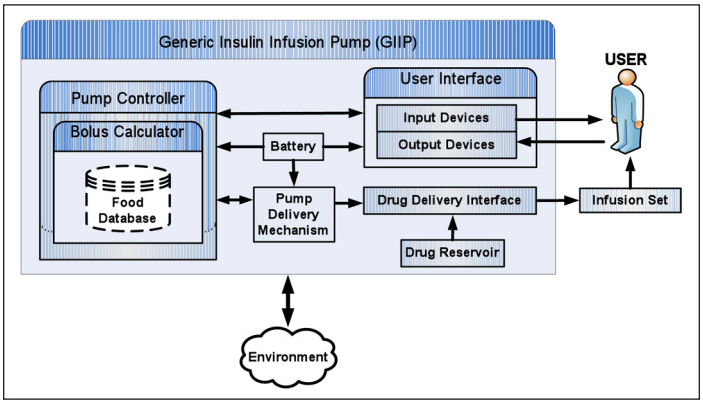

Figure 1. System architecture of generic insulin infusion pump.

We focus our analysis on software-driven functionality. Hardware issues are raised in only the broadest sense because our insulin pump model has no concrete notion of hardware. For example, we raise the issue of electromagnetic interference as a source of hazards, but offer no in-depth causes of it.

Caveats

The GIIP model is composed of various abstract functional components consistent with the stated scope. There is probably no single device currently on the market that has all of the design features and subsequent safety issues represented in this model. For example, not all insulin pumps provide a food database feature. This feature was included in our model because it may become a common feature and its use (or lack of use) presents risks that should be considered in a hazard analysis.

The hazard analysis results presented are not considered to be exhaustive. An in-depth fault tree analysis[7] and hazard and operability analysis[8] remain to be performed. Additionally, a compendium of use cases is needed to challenge the model architecture and component interaction. By performing these activities it is likely that additional sources of hazardous situations will be revealed. However, these activities are beyond the scope of this article.

Manufacturers who reference this generic analysis in their design process may benefit from checking their results against this independent work. Manufacturers claiming to use this preliminary hazard analysis in their design process still have to establish sufficient evidence to the FDA that their device is safe and effective.

Generic Insulin Infusion Pump Architecture

The GIIP administers insulin to the user via a delivery path, composed of a drug reservoir, a drug delivery interface, and the infusion set. Along this path, the drug reservoir acts as a built-in storage unit for insulin that will be monitored and administered. The drug delivery interface represents a segment of concealed tubing connecting insulin flow from the reservoir to the infusion set. A pump delivery mechanism provides the force for moving insulin from the pump to the user at a prescribed rate and for a prescribed duration.

The user/patient interacts with the GIIP through the GIIP user interface. The user interface allows the user to receive information from GIIP output devices and input data/commands through GIIP user input devices.

The environment (cloud) is constrained to physical properties such as temperature, pressure, sound, and radiation energies. (Examples of exclusions are enumerated earlier, in the *Scope* section of this article.)

The pump controller component represents an abstraction of generic insulin pump software. It provides the operational "glue" and robustness in the GIIP system. To ensure correct and timely insulin administration, the controller should be able to perform at least the basic functions listed here:

- Interpret user commands and inputs received from user input devices and act appropriately
- Maintain user-defined insulin delivery profiles
- Recommend appropriate boluses to correct low BG levels or cover future meals based on parameters entered by the user
- Encode and send instructions to the pump delivery mechanism such that it can precisely administer insulin based on user-defined insulin delivery profiles
- Send information to output devices allowing the user to monitor the status of the pump or of the current delivery session
- Instruct output devices to issue user-perceivable alarms and alerts
- Record important data and events during pump use to facilitate clinical statistics and problem diagnosis

Pump controller bolus recommendations present special risk considerations. Such a feature saves users the trouble of calculating bolus doses manually, potentially reducing calculation errors. Conversely, user trust in an incorrectly computed bolus recommendation can cause a hazardous situation. We have introduced a bolus calculator subcomponent as part of the pump controller to help draw proper attention to the safety critical nature of this function.

Another safety issue related to bolus recommendation is the increasing use of food databases by modern insulin pumps. These databases contain nutritional facts about typical food portions (e.g., carbohydrates). Pumps with this feature can assist the user in estimating the amount of carbohydrates contained in a meal. This information can be used in determining an appropriate insulin bolus. We felt it reasonable to incorporate a food database subcomponent in our GIIP model because inaccuracy or incorrectness here can affect correct bolus recommendations, and thus patient safety.

To make our PHA less ambiguous, we assume that only the following four types of insulin administrations can be programmed into or requested from the GIIP:

1. Basal provides background insulin replacement, delivered as a low, continuous infusion of insulin, periodically over a 24-hour interval.
2. Temporary basal provides insulin in proportion to physical conditions and activity levels of the user. Once programmed, a temporary basal overrides any ongoing normal basal at user-specified rates for user-indicated durations.
3. Normal bolus provides a user-defined amount of insulin immediately for covering food intake or correcting high BG levels.
4. Extended bolus is similar to normal bolus but is delivered over a period designated by the user.

Dual boluses that many insulin pumps support can be modeled as a normal bolus followed by an extended bolus.

Preliminary Hazard Analysis

The preliminary hazard analysis provided in the **Appendix** is based on four sources of information:

1. Domain knowledge from manufacturers, pump users, and clinicians
2. Adverse event reports collected by the FDA
3. Workshops sponsored by the Diabetes Technology Society[9,10]
4. International Organization for Standardization (ISO) 14971[2]

When receiving therapy from an insulin pump, a user might encounter various hazardous situations in which her/his health is at risk. A hazardous situation, according to the ISO 14971 standard, is a circumstance in which people, property, or the environment is exposed to one or more

hazards, where a hazard represents a potential source of harm (i.e., physical injury or damage to the health of people, or damage to property or the environment[2]). Overdose and underdose are the most likely hazardous situations in insulin pump use resulting in hypoglycemia or hyperglycemia, respectively. In an overdose or underdose situation, the patient receives more (or less) insulin administration from the pump than required to maintain desirable BG levels.

Hazardous situations for the GIIP model are summarized in **Table 1** of the **Appendix**. They are broadly categorized in terms of therapeutic, energetic, biological/chemical, mechanical, and environmental.

The creation of a hazardous situation is contingent on certain conditions or combinations of conditions being realized during operation of the pump. An underdose, for instance, can be caused by air bubbles getting into the delivery path (air in line) of the pump. The presence of air bubbles can be caused by many factors, such as design defects, manufacturing flaws, device failures, misconnections, and use errors.

Tables 2 through **9** in the **Appendix** identify a generic set of hazardous situations, their causes and contributing factors, and implicit cause–effect relations among these entities. To facilitate traceability, we categorize the analysis in terms of engineering design considerations, as follows:

- Operational sources of hazardous situations (**Table 2**)
- Software sources of hazardous situations (**Table 3**)
- Hardware sources of hazardous situations (**Table 4**)
- Physical sources of hazardous situations (**Table 5**)
- Electrical sources of hazardous situations (**Table 6**)
- Biological and chemical sources of hazardous situations (**Table 7**)
- Use sources of hazardous situations (**Table 8**)
- Environmental sources of hazardous situations (**Table 9**)

Each row in the tables establishes a cause–effect relationship (causal chain). This relationship is established in terms of an identified primary cause, the associated hazardous situation(s) resulting from the primary cause, and, when possible, all contributing factors to the primary cause. These tables represent an aggregation of causal chains. If one were to diagram these tables graphically, a tree-like structure would emerge. We refer to this tree-like structure as a causal tree. It should be noted that the tabular-based causal tree structure presented here represents just one of many arbitrary ways to organize a hazard analysis.

Discussion

Rationale for PHA Table Organization

Terms associated with a hazard analysis such as hazard, hazardous situation, and event (cause, contributing factor) are rather ambiguous and their description often arbitrary. For example, consider leakage of insulin from the delivery path. Such an event, if left undetected, could cause an underdose hazardous situation. The event could also cause an incorrect calculation of the amount of insulin to be delivered, which in turn will cause an incorrect calculation of future boluses resulting in an under/overdose hazardous situation. Is the leakage a cause or contributing factor of incorrect future boluses or the initiating event of a sequence of events leading to underdose? The ambiguity in terminology further exacerbates analysis when different levels of design abstraction are being considered. What seems more important than resolving terminology issues is the application of some disciplined method for assessing how a particular design can cause harm.

We assemble cause–effect relations identified in our analysis into an aggregated tabular causal tree. Each edge represents a particular cause–effect relation consisting of two levels: (a) a primary cause and (b) contributing factors to the cause. Cross-cutting edges can exist between branches in the tree. Clearly, cause–effect relations resulting in hazardous situations can be quite complex, even in our rather simple abstract pump architecture.

The comprehensiveness of the hazard analysis depends, in part, on the level of design abstraction. As more implementation details are established, additional causes of hazardous situations are manifested. In our GIIP model, no assumption is made about how pump components are implemented or assembled with other components. Nevertheless, the safety-related issues established here can be mapped easily to most real-world insulin pump implementations because the analysis is at a high system level.

Using and Extending PHA Tables

Specific insulin pump devices may or may not have design features that are instantiated from the GIIP safety model. Manufacturers using our PHA results in their development process should consider the following criteria:

1. If certain design features included in the GIIP are not implemented in the device, related causes or contributing factors are not applicable to the device and should be ignored.

2. If a design feature addressed by the GIIP is implemented in the device, relevant factors presented in the PHA tables can (and should) be used to assess the safety properties of the device. Any side or collateral effects introduced by the GIIP PHA should be appropriately considered and dealt with as well.

3. If the device includes a design feature outside the GIIP system boundary, then two possibilities need to be considered.

    i. The design feature can be modeled as a new component in the (necessarily expanded) GIIP system. Remote controllers, as now seen in use with some modern insulin pumps, provide an example of such a feature. If a new remote control component is incorporated in the GIIP model, analysis would then need to consider safety issues associated with this remote control component and its interactions with other GIIP components.

    ii. This design feature cannot be modeled as a new functional GIIP component, but it may affect the safety properties of one or more GIIP components. An example of this case is pump miniaturization, i.e., design or implementation efforts to make insulin pumps smaller and more compact. As a system-level feature, pump miniaturization will obviously affect all aspects of the device. If such a design feature is introduced, the PHA tables will likely need to be updated—eliminating elements invalidated by the new feature(s) and adding elements introduced by the new feature(s).

Human Factors Considerations

Referring to the **Appendix**, one causal factor worth calling special attention to is in **Table 8**, cause 8.10.13, which deals with "human factors issues." It is meant to be a placeholder for all possible pump-user interface issues that can affect users' easy, safe, and comfortable use of the device. Because of a lack of design and implementation details, we do not elaborate on this particular cause in the analysis. However, we encourage manufacturers to analyze their pump-user interface design comprehensively and correct any design feature that does not comply with the intended users of their devices. In order to do this, manufacturers need to identify the user population of their devices; fully understand physical, psychological, social, cultural, and biological characteristics of the population; and apply this understanding in the analysis. For example, if an insulin pump is intended to be used by senior citizens, then it should not incorporate a small display with unreadable fonts or a keypad with buttons bearing small symbols that cannot be read or interpreted easily. More broadly, the notion of information overload merits special attention. In this situation, the pump can be performing correctly, but the user becomes overwhelmed by all the information being presented and ultimately does something incorrect.

Mobility Considerations

Advances in insulin pump design permit greater user mobility, which in turn is believed to improve the user's quality of life. This "mobility" property can cause the pump to be exposed to environmental conditions that can affect pump operation and patient safety. In the home use environment, the pump might be exposed to electromagnetic emissions from cell phones, microwave ovens, or even other medical devices that could upset device operation. Similarly, exposure to X-rays (airport security), radio frequency identification readers, magnetic resonance imaging (medical imaging), or combinations of radiations is possible. The mobility property might encourage the user to use an insulin pump in environments that have subtle safety implications. A camping site is an example of such an environment—there may be limited user access to sufficient pump supplies, such as batteries, insulin, or infusion sets.

Mobility factors can often affect the design of multiple device components in subtle ways. If miniaturization is used as a means of improving mobility, the pump might become more susceptible to electromagnetic disturbances or other types of radiations or introduce new circuit design issues. Manufacturers need to give careful thought to possible hazardous situations caused by pump mobility factors.

Our PHA addresses a number of mobility conditions, but is not exhaustive. This is in part due to the level of

device abstraction being modeled. We enumerate some additional mobility conditions here that warrant special consideration as part of a comprehensive hazard analysis:

- Effects on pump or insulin due to temperature extremes
- Flow rate deviation due to ambient air pressure fluctuations
- Exposure to radiation
- Accidental disconnections of infusion sets due to outdoor activities
- Water ingress (shower at home, swimming at beach)
- User missing alarms or alerts due to ambient noises
- Exposure to pathogens, allergens, or other infectious substances
- Inaccessibility to pump supplies due to outdoor activities
- Time-of-day discrepancy due to long-distance travels (e.g., time zone changes)

Conclusion

This article introduced a generic insulin pump model and a preliminary hazard analysis based on this model. The model is an abstraction of real-world insulin pumps, encapsulating common design features. Issues such as the selection and integration of electrical, material, mechanical, and chemical elements are not relevant to the abstraction. Rather, we concern ourselves with system-level safety issues that are manifested at the pump user interface.

We believe that there is considerable value in having the diabetes and academic communities and manufacturers consider and discuss these preliminary hazards in order to extend them, to make them more complete, to experiment with them, and to reference them in insulin pump designs. By doing so in an open forum, it may be possible to establish an open system insulin pump safety reference model that can be most helpful in improving the safety and effectiveness of insulin pumps and in streamlining the regulatory process for placing them on the market. We encourage those interested in establishing such a reference model to contact the authors.

Acknowledgment:

The authors thank the following people for their contributions to this article:

ASHVINS Group Technology Professionals
Lynn Hilt, Thomas Love and Alin Andea
Miami, Florida

David C. Klonoff, M.D., FACP
Medical Director, Diabetes Research Institute
Mills-Peninsula Health Services
San Mateo, California

Lt Col Mark W. True, M.D., FACP, FACE
Director, Diabetes Center of Excellence
Lackland Air Force Base
San Antonio, Texas

Nugget Burkhart, B.S.N., M.A., NP, BC-ADM, CDE
Diabetes Care Manager, Department of Medicine
Kaiser Permanente Medical Center
San Francisco, California

Meaghan Devlin, R.N.
Staff Nurse
Massachusetts General Hospital
Boston, Massachusetts

Tamara James, R.N., CDE
Clinical Resource Nurse III
UC Davis Medical Center
Sacramento, California

Elizabeth Kunselman, NP, CDE
Lucile Packard Children's Health Services
Stanford University Medical Center
Stanford, California

Irina Nayberg, R.N., B.S.N., CDE
Clinical Research Coordinator
Mills-Peninsula Health Services
San Mateo, California

Gloria Yee, R.N., CDE
Principal Diabetes Instructor
Diabetes Teaching Center, UC San Francisco
San Francisco, California

References:

1. Diabetic Control and Complications Trial Research Group. The effect of intensive treatment of diabetes on the development and progression of long-term complications in insulin-dependent diabetes mellitus. N Engl J Med. 1993;329(14):977-86.
2. ISO 14971. Medical devices--application of risk management to medical devices; 2007.
3. FDA MAUDE database. Available from: http://www.accessdata.fda.gov/scripts/cdrh/cfMAUDE/search.CFM.
4. Kampfner RR. Model-based development of computer-based information systems. Proceedings of the Workshop on Engineering of Computer-Based Systems (ECBS); 1997. p. 354.
5. Arney D, Jetley R, Jones P, Lee I, Sokolsky O. Formal methods based development of a PCA infusion pump reference model: generic infusion pump (GIP) project. 2007 Joint Workshop on High Confidence Medical Devices, Software, and Systems and Medical Device Plug-and-Play Interoperability. p. 22-33.

6. Generic PCA infusion pump safety model. Available from: http://rtg.cis.upenn.edu/gip.php3.
7. U.S. Nuclear Regulatory Commission Fault Tree Handbook (NUREG-0492). Available from: http://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr0492/sr0492.pdf.
8. British Standard BS: IEC61882:2002 Hazard and operability studies (HAZOP studies).
9. Klonoff DC, Reyes JS. Insulin pump safety meeting: summary report. J Diabetes Sci Technol. 2009;3(2):396-402.
10. Zhang Yi, Jones PL, Klonoff DC. Second insulin pump safety meeting: summary report. J Diabetes Sci Technol. 2010;4(2):488-93.

Appendix

A user might confront various hazardous situations when receiving therapy from an insulin pump. **Table 1** provides a description of typical GIIP hazardous situations. These hazardous situations are usually contingent on certain causal events realized during operation of the pump. For example, underdose, i.e., the patient receives less insulin than expected, can be caused by air bubbles being introduced into the delivery path of the pump without his/her awareness.

Table 1.
Hazardous Situations Associated with GIIP

Category	Hazardous situation
1. Therapeutic	1.1 Overdose: the user receives more insulin than required to maintain desirable BG levels
	1.2 Underdose: the user receives less insulin than required to maintain desirable BG levels
	1.3 Incorrect treatment: the user receives either an incorrect drug or a correct drug with incorrect concentration
2. Energetic	2.1 Excessive thermal energy generation by the pump
	2.2 Electrical shock: the pump transfers electric current to accessible surfaces during operation
	2.3 Excessive electromagnetic emissions by the pump: affects the pump itself, other device(s) worn by the user, or other users and their devices
	2.4 Excessive sound frequencies generated by the pump
3. Chemical/biological	3.1 User infection
	3.2 User allergic reaction/rash to pump materials or insulin[a]
4 Mechanical	4.1 Presence of sharp edges or scissor points
	4.2 Excessive pump vibration, e.g., connectors, components stressed
5. Environmental	5.1 Unsafe disposal of the pump or pump components: user disposes batteries or other pump subassemblies in an unsafe manner

[a] The user may also be allergic to infusion set adhesives. However, because such adhesives have been excluded from the GIIP system, we do not consider hazardous situations related to infusion set adhesives here.

Appendix

Table 2.
Operational Sources of Hazardous Situations

ID	Primary cause	Hazardous situation[a]	Contributing factor
2.1	Air in line	1.2	Incorrect/incomplete priming processes
			User's motions cause the delivery path to be loose or broken
			Broken, loose, or unsealed delivery path
			Pump or pump components are unable to release gas or air
			Cold insulin is loaded and then warms up to form air bubbles
			Pump is connected with incompatible infusion sets
2.2	Free flow	1.1	Valves in the delivery path are broken
			Air pressure within the pump is much lower/higher than ambient air pressure
			Pump is positioned much higher than the infusion site, causing unintentional drug flow
			Delivery path is damaged, creating a vent on the path that allows unintentional gravity flow
			Large temperature changes causing a mismatch between drug reservoir volume change and insulin density change
2.3	Reverse flow	1.2	Siphon effect due to the pump being positioned much lower than the infusion site
			Delivery path is damaged, creating a vent on the path that diverts an intentional drug flow from reaching the user
			Pump delivery mechanism runs opposite to the expected direction
			Air pressure within the pump is much lower/higher than ambient air pressure
2.4	Pump is disconnected from the infusion set without the user's awareness	1.2	User's motions cause the pump or the attached infusion set to be disconnected from the user
			Loose connection between parts of the delivery path
			Infusion set is not applied to the user correctly or is caught on the infusion set adhesives or tapes, causing it to be disconnected from the user
2.5	Excessive bolus administration due to too many bolus requests from the user	1.1	Bolus history is corrupted, making the user unable to track previous boluses
			User forgets about previously received boluses and requests additional unnecessary boluses without consulting the bolus history records
			User requests a meal bolus but does not eat
2.6	Occlusion without the user's awareness	1.2	Delivery path obstruction, e.g., kinked tubes
			Chemical precipitation inside the delivery path
2.7	Dosage of bolus is delivered unevenly over its specified duration	1.1, 1.2	Algorithmic errors
			Pump delivery mechanism does not operate as instructed

Continued →

Appendix

Table 2. Continued

ID	Primary cause	Hazardous situation[a]	Contributing factor
2.8	Insulin leakage	1.2, 3.1, 3.2	User does not follow instructions to disconnect the pump appropriately
			Pump is disconnected without the user's awareness
			Loose connection between parts of the delivery path
			Broken drug reservoir
			Occlusion during insulin delivery causes high pressure within the delivery path
2.9	Drug reservoir becomes empty during insulin delivery without the user's awareness	1.2	
2.10	Insulin level in the drug reservoir becomes low during insulin delivery without the user's awareness	1.2	
2.11	Actual flow rate does not match the programmed infusion rate	1.1, 1.2	Occlusion without the user's awareness
			Air pressure within the pump is much lower/higher than ambient air pressure
			Outside temperature is out of safe range or fluctuating inadvertently, causing the pump to deliver insulin inaccurately or behave erratically
			Outside air pressure is out of safe range or fluctuating inadvertently, causing the pump to deliver insulin inaccurately or behave erratically
			Electromagnetic interference due to internal or external electromagnetic disturbances, causing the pump to deliver insulin inaccurately or behave erratically
2.12	Excessive flow rate fluctuation	1.1, 1.2	
2.13	A replaceable drug reservoir is detached during normal pump use	1.2	Drug reservoir compartment is broken or opened
			User's motions cause the reservoir to be disconnected
2.14	Unexpected delivery of insulin	1.1	Software instructs to resume a previous bolus after suspension, or after the battery is replaced, causing an unexpected bolus
			Software instructs pump to finish paused basal delivery after a long suspension/interruption, causing a huge bolus to be flushed to the user
			User is connected to the pump while it is being refilled or primed
			User is connected to the pump while freeing clogged infusion tubes or detaching the reservoir
			Releasing occlusion causes unexpected boluses
			Large temperature changes causing a mismatch between the drug reservoir volume change and the insulin density change
			Pump fails to shut off or stop insulin delivery as commanded, and the user is not aware of this
2.15	Pump stops delivering insulin without the user's awareness	1.2	Pump suspends or stops without the user's awareness
			Drug reservoir is loaded improperly, causing no insulin to be delivered
2.16	Pump hardware is not initialized properly	1.1, 1.2, 1.3	Pump platform fails to meet default operational specifications

[a] This column is populated with links to entries in **Table 1**.

Appendix

Table 3.
Software Sources of Hazardous Situations

ID	Primary cause	Hazardous situation	Contributing factor
3.1 Inappropriate bolus is recommended by the bolus calculator and then accepted by the user			
3.1.1	Incorrect meal bolus is recommended by the bolus calculator	1.1, 1.2	User estimates or enters carbohydrate content of a planned meal incorrectly
			Food database contains erroneous information, causing incorrect calculation of the number of carbohydrates in a meal
			User determinates or enters carbohydrate ratios (food factors) incorrectly
			User misunderstands reverse correction or does not use reverse correction upon appropriate conditions Reverse correction refers to an optional feature that automatically adjusts meal bolus recommendations when the user encounters low BG levels. In particular, if this option is chosen, then calculation of a meal bolus dose, when the user's current BG level is below the target BG level, should reduce the amount of insulin necessary to bring the BG level back to target. This contributing factor is applicable only if the pump supports reverse correction.
			Design flaws/implementation defects in the bolus calculator
			Unexpected software execution
3.1.2	Incorrect correction bolus is recommended by the bolus calculator	1.1, 1.2	Pump provides the user only limited flexibility, such as coarse increment steps, to input parameters critical to bolus calculation
			Inappropriate or incorrect calculation of insulin on board (IOB)
			User estimated or entered his/her sensitivity to insulin over time (correction factors) incorrectly
			Calculator uses obsolete BG readings as the user's current BG level to calculate correction bolus
			User measured or entered BG values incorrectly
			User estimated or entered target BG levels incorrectly
			Design flaws/implementation defects in the bolus calculator
			Unexpected software execution
3.1.3	Inappropriate or incorrect calculation of IOB	1.1, 1.2	Pump provides the user limited or no capability to configure the duration of insulin action (DIA), causing input DIA to not be accurate enough for correct IOB calculation
			User injects insulin manually, which is not accounted for by the pump when calculating IOB
			Insulin leakage, causing the pump to miscalculate the amount of IOB
			Records of previous boluses become corrupt due to memory corruption or become inconsistent due to pump time changes
			Design flaws/implementation defects in the bolus calculator
			Unexpected software execution
3.2	Pump unexpectedly restores to default factory settings without the user's awareness	1.1, 1.2	User inadvertently selects a restore of the factory settings
			Accumulated static electricity during use triggers an unexpected restore of default factory settings
			Battery is inadvertently disconnected from the pump

Continued →

Appendix

Table 3. Continued

ID	Primary cause	Hazardous situation	Contributing factor
3.3	Pump controller fails to monitor the status of the pump delivery mechanism	1.1, 1.2	
3.4	Pump controller fails to detect mechanism failures of pump delivery	1.1, 1.2	
3.5	Pump annunciates notifications of different importance to the user with similar signals	1.1, 1.2	
3.6	Pump presents inappropriate or inaccurate prompts to the user	1.1, 1.2, 1.3	
3.7	Incorrect critical data. Data critical to insulin delivery include correction factors, food factor, basal infusion profiles, programmed bolus deliveries, records of previous insulin deliveries, BG logs, and target BG levels, as well as information about loaded insulin and food database (if applicable)	1.1, 1.2, 1.3	Data tampered with by unauthorized personnel
			Data corrupted due to memory corruption
			User provides the pump with incorrect, inaccurate, or incomplete information
			Pump does not record insulin delivered to the user during the period the user chooses to disconnect the pump and actual disconnection
			Insulin leakage, resulting in incorrect records of previous insulin deliveries
3.8	Corrupted infusion commands	1.1, 1.2	Data tampered with by unauthorized personnel
			Random-access memory or nonvolatile memory failure, including failing to write to memory, failing to read from memory, and memory corruptions
			Watchdog error
			Software defects, e.g., stack overflow, pointer corruption, math overflow, race conditions
3.9	Incorrect or inappropriate basal profiles are programmed/activated	1.1, 1.2, 1.3	Pump only provides limited options for the user to configure correction factors
			Pump provides limited or no flexibility for the user to program basal delivery profiles to compensate for different behavior patterns
			Pump does not display necessary details about basal profiles on the user interface, e.g., time of latest modification, causing the user to activate an inappropriate basal profile
3.10	Unexpected software execution	1.1, 1.2	Software update error or failure
			Software defects, e.g., stack overflow, pointer corruption, math overflow, race conditions
			Operating systems and/or runtime supports corrupted, failed, or updated
			Hardware failure, e.g., central processing unit (CPU), memory, input/output (I/O), "bus," power glitch, radiation/electromagnetic interference (EMI)
3.11	Data logging/retrieval failure	1.1, 1.2	
3.12	Inappropriate setting of alarm priorities	1.1, 1.2	
3.13	Pump fails to auto-stop upon detecting a critical failing condition that requires it to stop	1.1, 1.2	

Continued →

Appendix

Table 3. Continued

ID	Primary cause	Hazardous situation	Contributing factor
3.14	Inadequate or overcomplicated operating instructions	1.1, 1.2, 1.3	
3.15	Software not initialized to appropriate values	1.1, 1.2, 1.3	During pump startup, reset, power-off/power-on sequence software is not initialized to appropriate values
3.16	Nuisance alarming	1.1, 1.2, 1.3	Inappropriate setting of alarm priorities
			Sensor failures
3.17	Pump unexpectedly resets to default pump settings without the user's awareness	1.1, 1.2	User inadvertently selects a device reset
			Accumulated static electricity during use triggers an unexpected reset of the device
			Battery is inadvertently disconnected from the pump, triggering a reset
			Hardware failure, e.g., CPU, memory, I/O, "bus," power glitch, radiation/EMI

Table 4.
Hardware Sources of Hazardous Situations

ID	Primary cause	Hazardous situation	Contributing factor
4.1 Computational infrastructure issues			
4.1.1	Central processing unit failure	1.1, 1.2	
4.1.2	Random-access memory or nonvolatile memory failure, including failing to write to memory, failing to read from memory, and memory data corruptions	1.1, 1.2	
4.1.3	Read-only memory or external flash memory failure	1.1, 1.2	
4.2 Motor issues			
4.2.1	Pump delivery mechanism does not operate as instructed	1.1, 1.2	
4.2.2	Pump delivery mechanism fails and does not stroke	1.2	
4.2.3	Fail to stop the motor of the pump when a fault condition occurs	1.1, 1.2	
4.2.4	Fatigued/worn/broken mechanical parts	1.1, 1.2, 2.1, 4.2	
4.3 User interface issues			
4.3.1	User interface components of the pump, including display units and alarming units, fail or behave abnormally	1.1, 1.2, 1.3	
4.3.2	Input device, e.g., keypad or touch screen, does not work correctly	1.1, 1.2, 1.3	
4.3.3	Key bounce not detected or corrected	1.1, 1.2, 1.3	
4.3.4	Key stuck	1.1, 1.2, 1.3	

Continued →

Appendix

Table 4. Continued

ID	Primary cause	Hazardous situation	Contributing factor
4.3.5	Audio notifications or prompts cannot be heard in a normal use environment	1.1, 1.2, 1.3	Defective audio device(s)
			Incorrect audio volume settings
4.3.6	Audio notifications or prompts too loud	2.4	Abnormal audio device(s)
			Incorrect audio volume settings
4.3.7	Delayed alarm detection and notifications	1.1, 1.2, 1.3	Sensor problems
			Software errors
4.3.8	Nonaudio alarm cannot be seen/interpreted	1.1, 1.2, 1.3	Light-emitting diode failure
			Color blindness
			Poor location
4.3.9	Nonaudio alarm cannot be felt (vibration)	1.1, 1.2, 1.3	Vibration mechanism fails
			Incorrect vibration setting
			Pump location
4.4 Pump housing issues			
4.4.1	Inadequate electrical/radiation shielding for the pump	2.2, 2.3	
4.4.2	Improper shape design or improper manufacturing process	2.3,4.1	
4.5 Sensors and watchdog[a] issues (applicable only if the pump integrates sensors and independent watchdogs)			
4.5.1	Sensor failure	1.1, 1.2, 1.3	
4.5.2	False watchdog interrupt	1.1, 1.2, 1.3	
4.5.3	Watchdog timer failed; watchdog does not interrupt as expected	1.1, 1.2, 1.3	
4.6 Other hardware issues			
4.6.1	Time base, such as real-time clock (RTC), used by the pump to control insulin delivery speeds up, slows down, or stalls	1.1, 1.2	
4.6.2	System RTC not synchronized (date/time register not the same as the RTC)	1.1, 1.2	
4.6.3	Synchronization error between pump components	1.1, 1.2	
4.6.4	Component communication/bus/channel failure	1.1, 1.2	
4.6.5	Broken drug reservoir	1.2	

[a] A watchdog is typically a software/hardware component that can cause the system to reset when it judges that the system either has paused too long or is no longer performing the expected behavior due to abnormal conditions.

Appendix

Table 5.
Physical Sources of Hazardous Situations

ID	Primary cause	Hazardous situation	Contributing factor
5.1	Physical damage to the pump or its sub-assemblies.	1.1, 1.2, 2.3, 4.1	User drops the pump accidentally
			Pump is sheared due to contact with surrounding surfaces or objects
			Excessive external stress is applied to the pump
5.2	Fluid/humidity ingress into the pump	1.1, 1.2, 2.1, 2.2	
5.3	Air pressure within the pump is much lower/higher than ambient air pressure	1.1, 1.2	Pump fails to equalize internal and external air pressure
			Pump develops internal vacuum as insulin is delivered
			Outside air pressure is out of safe range or fluctuating inadvertently, causing the pump to deliver insulin inaccurately or to behave erratically
			Temperature inside the pump is out of safe range or fluctuating inadvertently, causing the pump to deliver insulin inaccurately or to behave erratically
5.4	Pump overheats while running	1.1, 1.2	Mechanical failures
			Electrical failures

Appendix

Table 6.
Electrical Sources of Hazardous Situations

ID	Cause	Hazardous situation	Contributing factor
6.1	Nonfunctioning/disabled electrical circuits/components, e.g., shorted electrical circuits.	1.1, 1.2, 2.1, 2.2	Electrical circuit/component failures
			Fluid/humidity ingress
6.2	Erratic electric circuit operations	1.1, 1.2, 2.3	Nonfunctioning/disabled electrical circuits/components, e.g., shorted electrical circuits
			Pump develops excessive static charge or experiences electrostatic discharge (ESD) that exceeds its ESD immunity
			Fluid/humidity ingress into the pump
			Voltage level of the battery is too low
			Voltage level of the battery varies greatly
			Battery impedance or contact impedance becomes too high
			Electromagnetic interference
6.3	Pump develops excessive static charge or experiences ESD that exceeds its ESD immunity	1.1, 1.2	Pump is rubbing against surrounding surfaces or articles
6.4	Leakage current on the surface of the pump	2.2	
6.5 Battery-related issues			
6.5.1	Battery depletes without the user's awareness	1.2	
6.5.2	Battery depletes rapidly, giving the user insufficient time to respond	1.2	
6.5.3	Voltage level of the battery is too low	1.1, 1.2	
6.5.4	Voltage level of the battery varies greatly	1.1, 1.2	
6.5.5	Battery life is unpredictable	1.1, 1.2	
6.5.5	Battery is inadvertently disconnected from the pump	1.2	Broken battery compartment or broken battery compartment cap
			User drops the pump accidentally, disconnecting the battery temporarily
6.5.7	Battery impedance or contact impedance becomes too high	1.1, 1.2	
6.5.8	Depleted batteries are discarded without being recycled	5.1	

Appendix

Table 7.
Biological and Chemical Sources of Hazardous Situations

ID	Primary cause	Hazardous situation	Contributing factor
7.1	Pump, especially its delivery path, is contaminated with toxic substances	3.2	Inadequate pump cleaning/sterilization (e.g., residue after contamination, failure to flush, failure to disinfect)
			Battery fluid or other fluid leaks into the delivery path
			User uses inappropriate cleaning agents while cleaning the pump routinely
			User keeps using the pump for a period longer than recommended
7.2	Pump is exposed to pathogens, allergens, and other infectious substances	3.1	Pump is shared by multiple users
			Packaging of the pump is damaged prior to its use, but the user applies the pump regardless
			Inadequate pump cleaning/sterilization, such as residue after contamination, failure to flush, and failure to disinfect, causing the pump to lose its sterility
			Pump is connected to nonsterile infusion sets
7.3	Chemical precipitation inside the delivery path	1.2, 3.2	Incorrect/incomplete pump cleaning procedure
7.4	Infusion site infection	3.1	User fails to clean the infusion site completely before applying the infusion set
			User fails to change infusion sites as recommended
7.5	Insulin, while being delivered to the user, loses its potency	1.3	Insulin contacts with incompatible pump material
			Environmental temperature is too high/low
7.6	Pump is made of materials that cause user allergic reactions	3.2	

Appendix

Table 8.
Use Sources of Hazardous Situations

ID	Primary cause	Hazardous situation	Contributing factor
8.1	User uses the pump when certain physical/mental conditions such as impaired vision prevent him/her to do so	1.1, 1.2, 1.3	
8.2	User is incapable of using the pump or configuring treatment plans	1.1, 1.2, 1.3	User is not sufficiently trained to operate the pump; user is not sufficiently intelligent to understand the instructions and use the pump correctly
			User falls asleep or goes into coma due to hypoglycemia
8.3	User injects long-acting insulin shortly before first use of the pump, causing an amount of insulin on board that cannot be accounted for by the pump	1.1	
8.4	User is connected to the pump incorrectly	1.1, 1.2	
8.5	User fills the pump with wrong types of insulin, degraded insulin, or drugs other than insulin	1.3	
8.6	User fails to test his BG levels as frequently as recommended	1.1, 1.2, 1.3	
8.7	User travels to a different time zone and forgets to accommodate so-caused time discrepancy while using the pump	1.1, 1.2	
8.8	User fails to replace consumed pump supplies, including insulin and batteries, in time	1.2	User fails to attend to pump notifications
			User has no access to backup pump supplies
8.9 User provides the pump with incorrect, inaccurate, or incomplete information			
8.9.1	User inputs incorrect drug type and concentration information for currently loaded insulin	1.3	
8.9.2	User enters incorrect parameters when configuring basal profiles	1.1, 1.2	
8.9.3	User enters incorrect parameters when programming temporary basal deliveries	1.1, 1.2	
8.9.4	User measures or enters BG values incorrectly	1.1, 1.2	
8.9.5	User provides incorrect parameters to the bolus calculator. These parameters include the user's insulin sensitivities and corresponding effective periods; insulin-to-carbohydrate ratios and corresponding effective periods; the user's target BG levels and corresponding effective periods; and insulin duration of action	1.1, 1.2	
8.9.6	User estimates carbohydrate content of planned meals incorrectly	1.1, 1.2	User guesses, instead of consulting with food database, the number of carbohydrates in the meal
			User specifies incorrect categories or amounts of ingredients in the meal

Continued →

Appendix

Table 8. Continued

ID	Primary cause	Hazardous situation	
8.10 User interacts inappropriately with the user interface of the pump			
8.10.1	User touches the input units of the pump accidentally, causing unintentional changes on pump settings, pump states, or insulin delivery programs	1.1, 1.2	
8.10.2	User interacts improperly with the input mechanisms of the pump, e.g., pressing the keypad for too long or not long enough, causing the pump to misinterpret the user's intention	1.1, 1.2	
8.10.3	User fails to confirm revisions on insulin delivery programs, leaving the pump unchanged without his/her awareness	1.1, 1.2	
8.10.4	User forgets to confirm his/her action of activating another basal profile, leaving the current basal profile to continue without his/her awareness	1.1, 1.2	
8.10.5	User forgets to confirm his/her action of starting or stopping a temporary basal, a normal bolus, or an extended bolus	1.1, 1.2	
8.10.6	User commands a bolus to cover a meal but does not eat	1.1, 1.2	
8.10.7	User eats but forgets to bolus	1.2	
8.10.8	User commands boluses without consulting with the bolus calculator or inappropriately overrides boluses recommended by the bolus calculator	1.1, 1.2	
8.10.9	User inappropriately cancels a bolus in middelivery	1.1, 1.2	User misunderstands suggestions from the bolus calculator
			User stops a bolus due to false symptoms of hypoglycemia
8.10.10	User forgets to resume after suspending the pump	1.2	
8.10.11	User programs a special basal profile targeted at certain occasions, but forgets to activate this profile when targeted occasions occur	1.1, 1.2	
8.10.12	User fails to attend to pump notifications	1.1, 1.2, 1.3	Human factors issues
			Excessive background noise
			Outside lighting condition prevents the user from interacting with the pump correctly
			User muffles the speaker of the pump or other audio devices, either intentionally or unintentionally
			User disregards pump notifications intentionally
			"Nuisance" or false notifications occur too often and are subsequently ignored by the user
			User falls asleep or goes into coma due to hypoglycemia
8.10.13	Human factors issues	1.1, 1.2, 1.3	Information overload

Appendix

Table 9.
Environmental Sources of Hazardous Situations

ID	Primary cause	Hazardous situation	Contributing factor
9.1	Outside temperature is out of safe range or fluctuating inadvertently, causing the pump to deliver insulin inaccurately or to behave erratically	1.1, 1.2, 1.3	
9.2	Outside air pressure is out of safe range or fluctuating inadvertently, causing the pump to deliver insulin inaccurately or to behave erratically	1.1, 1.2, 1.3	
9.3	Electromagnetic interference	1.1, 1.2, 1.3	Inadequate immunity or mitigation
			Improper manufacturing process
			Failure to reinstall electromagnetic compatibility (EMC) components after service or reinstalling EMC components incorrectly
			Physical damage to the pump or its subassemblies
			Pump is used in the presence of electromagnetic disturbances that exceed its design specifications
9.4	Excessive background noise (preventing the user from attending to pump notifications)	1.1, 1.2, 1.3	
9.5	Outside lighting condition prevents the user from interacting with the pump correctly	1.1, 1.2, 1.3	
9.6	Unauthorized personnel tamper with pump configuration settings	1.1, 1.2, 1.3	
9.7	Unauthorized personnel tamper with information critical to insulin delivery	1.1, 1.2, 1.3	